

PATENT**Amendments to the Claims:**

Claims 1, 8, 15, 22 and 27 were amended. This listing of claims will replace all prior version, and listings, of claims in the application:

Listing of Claims:

- 1.(currently amended): A method for secure operation of a network device, comprising:
- (a) assigning a digital certificate to a network user;
 - (b) receiving a command for operation of a network device and the digital certificate from the network user;
 - (c) utilizing a cryptographic key stored in the network device to authenticate the digital certificate of the network user;
 - (d) enabling operation of the network device if the digital certificate of the network user is authenticated and if the operation is permitted by a usage policy associated with the network user; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy is at least one of a policy to ~~access~~ allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document.

2-4.(canceled)

PATENT

- 5.(original): The method as recited in claim 1, wherein the network user is another network device.
- 6.(original): The method as recited in claim 1, wherein the command for operation of the network device is encrypted, and wherein the cryptographic key is utilized to decrypt the command for operation.
- 7.(original): The method as recited in claim 1, further comprising receiving electronic payment for paying for operation of the network device.
- 8.(currently amended): A computer program embodied on a computer readable medium for secure operation of a network device, comprising:
- (a) a code segment embodied on the computer readable medium that assigns a digital certificate to a network user;
 - (b) a code segment embodied on the computer readable medium that receives a command for operation of a network device and the digital certificate from the network user;
 - (c) a code segment embodied on the computer readable medium that utilizes a cryptographic key stored in the network device to authenticate the digital certificate of the network user;
 - (d) a code segment embodied on the computer readable medium that enables operation of the network device if the digital certificate of the network user is authenticated and if the operation is permitted by a usage policy associated with the network user; and
- wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy is at least one of a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated

PATENT

with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document.

9-11.(canceled)

12.(original): The computer program as recited in claim 8, wherein the network user is another network device.

13.(original): The computer program as recited in claim 8, wherein the command for operation of the network device is encrypted, and wherein the cryptographic key is utilized to decrypt the command for operation.

14.(previously presented): The computer program as recited in claim 8, further comprising a code segment embodied on the computer readable medium that receives electronic payment for paying for operation of the network device.

15.(currently amended): A system for secure operation of a network device, comprising:

- (a) logic that assigns a digital certificate to a network user; and
- (b) a network device capable of receiving a command for operation thereof and the digital certificate from the network user, wherein the network device utilizes a cryptographic key to authenticate the digital certificate of the network user;
- (c) wherein operation of the network device is enabled if the digital certificate of the network user is authenticated and if the operation is permitted by a usage policy associated with the network user; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy is at least one of a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated

PATENT

with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document.

16-18.(canceled)

19.(original): The system as recited in claim 15, wherein the network user is another network device.

20.(original): The system as recited in claim 15, wherein the command for operation of the network device is encrypted, and wherein the cryptographic key is utilized to decrypt the command for operation.

21.(original): The system as recited in claim 15, further comprising logic that receives electronic payment for paying for operation of the network device.

22.(currently amended): A method for secure identification of a network device, comprising:

- (a) assigning a digital certificate to a network device;
- (b) receiving a command for operation of the network device from a network user;
- (c) sending the digital certificate to the network user, wherein the network user utilizes a cryptographic key to authenticate the digital certificate of the network device;
- (d) enabling operation of the network device if the digital certificate of the network device is authenticated and if the operation is permitted by a usage policy associated with the network user; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy is at least one of a policy to allow selection of special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated

PATENT

with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document.

23-24.(canceled)

25.(original): The method as recited in claim 22, wherein the network user is another network device.

26.(previously presented): The method as recited in claim 22, and further comprising assigning a unique digital certificate to a second network device, wherein the command for operation of the network device is re-routed to the second network device based on at least one of attributes of the network devices and the routing policy.

27.(currently amended): A method for secure management of a network device, comprising:

- (a) associating at least one of policy information and a computational protocol with a command for the network device;
- (b) encrypting the at least one of policy information and computational protocols;
- (c) sending the at least one of policy information and computational protocols to the network device;
- (d) decrypting the at least one of policy information and computational protocols;
- (e) processing the command with the network device utilizing the at least one of policy information and computational protocols; and

wherein the network device is at least one of a printer, a copier, a scanner, and a facsimile machine; and the usage policy is at least one of a policy to allow selection of access special paper stock, a policy to allow the network device to decrypt and print a document only if the network user was physically near the network device, a policy to print a selected watermark when printing the document, a policy to enable the network device to accept digital cash associated

PATENT

with an operation on the document, a policy to enable a billing function, a routing policy, and a policy to escrow a document.